Las Estrategias Electrónicas de China

Teniente Coronel (R) Timothy L. Thomas, Ejército de EE.UU.

EL GENERAL DE DIVISIÓN Dai Quinmin, director del Departamento de Comunicaciones del Estado Mayor General del Ejército de Liberación Popular de China y responsable de las operaciones de guerra de información y las operaciones de informática, recientemente escribió que: "las nuevas tecnologías probablemente encontrarán sus expresiones materiales en la forma de armas y equipo dotados de tecnologías de informática que, junto con sistemas de información, el sonido, la luz, la electrónica, el magnetismo, el calor y otros medios por el estilo, llegarán a constituir un portador de estrategias".[1] Las estrategias chinas dependen del empleo de electrones en formas imprevistas para llevar a cabo estratagemas tales como "matar con una espada prestada" y "agotar al enemigo invasor y atacarlo con calma".

Los chinos son de opinión que estrategias superiores pueden ayudarlos a superar sus deficiencias tecnológicas. Un equivalente comparable de este concepto teórico del arte militar sería un grupo virtual de maniobra operativo ruso, compuesto de fuerzas a base de electrones o bien un grupo de combate aeroterrestre electrónico de Estados Unidos.

El artículo de Dai es un hito importante en la filosofía del Ejército de Liberación Popular por varias razones. Primero, el autor es un personaje creíble y responsable. Antes de asumir su actual posición, Dai sirvió como comandante del Centro de Guerra de la Información del Ejército de Liberación Popular en Wuhan. Segundo, define la guerra de la información y las operaciones de información con características chinas, por lo cual estas definiciones son distintas de las estadounidenses. Tercero, Dai rompió con la tradición cuando abogó por la conducción de ataques preventivos para tomar la iniciativa y lograr la superioridad en el ámbito de las informaciones. Este énfasis en la ofensiva contradice la estrategia militar china que tradicionalmente se basa en la defensa activa. Finalmente, observó que la ejecución de operaciones de información conjuntas e integradas permite extender el alcance y propósito de la guerra popular. El artículo de Dai también indica que China está claramente desarrollando las estrategias adecuadas para implementar la guerra de información con características chinas. Otros escritores también defienden esta opinión con sus propias aproximaciones a la guerra de información a nivel estratégico.

El informe sobre China, preparado por el Secretario de Defensa de EE.UU. para el Congreso en el año fiscal 2000 (en cumplimiento de las disposiciones del Acta de Autorización de la Defensa Nacional), indicó adelantos tanto en las teorías como en las capacidades de los chinos. Dicho informe señala que desde el bombardeo no intencionado de la Embajada de China en Belgrado por parte de las fuerzas de la OTAN el 7 de mayo de 1999, los líderes chinos vienen acelerando el proceso de modernización de las Fuerzas Armadas, al mismo tiempo que se han abocado a iniciar negociaciones de cooperación estratégica con Rusia e incrementar sus actividades de proliferación. En particular, China se ha enfocado en contrarrestar a sus enemigos que posean avanzadas tecnologías de información y armas de precisión de largo alcance. Esta doctrina de "la defensa activa" se orienta hacia la "guerra popular bajo condiciones modernas", circunstancia que el informe del Secretario de Defensa describe como "guerras locales bajo condiciones de la alta tecnología".[2] El Libro Blanco sobre la Defensa China, publicado el día 16 de octubre de 2000, también puso de relieve la tradición de la guerra popular china, para sorpresa de muchos expertos occidentales en asuntos chinos que se habían convencido de que esta idea había perdido importancia en la era de la información. En realidad, su importancia ha crecido.

En el mes de septiembre de 2000, dos semanas antes de la publicación del Libro Blanco, en el diario el *PLA Daily* salió un artículo sobre la evolución de las telecomunicaciones en el sector militar chino. El artículo resaltó el hecho de que en 1991 el Presidente Jiang Zemin instó a que se esta-

blecieran sistemas de telecomunicaciones para uso civil y militar, capaces de satisfacer las necesidades de la población china en tiempos de guerra y de paz.[3] Sólo de esa forma sería posible que las telecomunicaciones militares avanzaran a la par con la industria comunicacional civil. Una manera de lograr lo anterior fue a través de la creación de fuerzas de reserva (un componente clave, que posibilita unir los sectores militar y civil en una guerra popular) con misiones de telecomunicaciones y de guerra de información /operaciones de información. Según consta en el Libro Blanco, "Hemos elaborado la estructura de una fuerza de reserva especializada en telecomunicaciones con un regimiento como unidad fundamental, basada en un departamento de informaciones del sector industrial . . . hemos construido un contingente de reserva integrado por personas capacitadas en los ámbitos de telecomunicaciones y transmisiones, cuya fuerza principal se compone de personas especializadas en telecomunicaciones repetidoras, digitales, telegráficas, por fibra óptica y por satélite . . . contando con al apoyo indispensable de un contingente de personal altamente capacitado incluyendo expertos en computación, peritos en el monitoreo de redes y unidades de telecomunicaciones por radio".[4]

Las fuerzas de reserva de China actualmente están dotadas de las armas adecuadas para cumplir misiones de guerra /operaciones de información, habiéndose convertido en el nexo que vincula la alta tecnología con la teoría de la guerra popular de esa nación. En el pasado, el papel previsto para las fuerzas de reserva era el de apoyar a las fuerzas del Ejército de Liberación Popular en defensa contra cualquier intervención extranjera. Las fuerzas de reserva de hoy tienen la capacidad para hacer algo que por muchos años quedaba fuera del alcance incluso del Ejército de Liberación Nacional: emplear armas electrónicas y de información para alcanzar a un adversario en otro continente. Los daños infligidos por un ataque electrónico pueden ser tan devastadores a la economía de una nación como lo son los efectos de un misil intercontinental.

La industria de defensa en China aún está atrasada en lo que dice relación con el desarrollo de equipo de alta tecnología; de ahí que China deba encontrar "focos selectivos de excelencia", de acuerdo con el fallecido líder nacional Deng Xiaoping. Uno de estos focos parece ser las telecomunicaciones internas. En el informe del Secretario de Defensa consta que las redes de comunicaciones civiles y militares pueden ser conectadas para ayudar a China en una crisis. Un informe publicado en el número de septiembre de la publicación *PLA Daily* indica que es más probable que se instituya un sistema de telecomunicaciones civil-militar. El sistema de comunicaciones militares se transmite en múltiples líneas para así maximizar su supervivencia, seguridad, flexibilidad, movilidad y resistencia a ataques electrónicos y a todo esfuerzo por explotarlo o destruirlo. Según dicen, la red automatizada de datos de comando puede apoyar varias opciones de ataques limitados convencionales planificados con antelación, en la periferia de China.[5]

El informe sobre China, preparado por el Secretario de Defensa de EE.UU. para el Congreso en el año fiscal 2000 . . . señala que desde el bombardeo no intencionado de la Embajada de China en Belgrado por parte de las fuerzas de la OTAN el 7 de mayo de 1999, los líderes chinos vienen acelerando el proceso de modernización de las Fuerzas Armadas, al mismo tiempo que se han abocado a iniciar negociaciones de cooperación estratégica con Rusia e incrementar sus actividades de proliferación. En particular, China se ha enfocado en contrarrestar a sus enemigos que posean avanzadas tecnologías de información y armas de precisión de largo alcance. Esta doctrina de "la defensa activa" se orienta hacia la "guerra popular bajo condiciones modernas", circunstancia que el informe del Secretario de Defensa describe como "guerras locales bajo condiciones de la alta tecnología".

También se informa que las fuerzas de reserva cuentan con sus propios *websites* y centros de simulación. China actualmente tiene 400 *websites* militares, según manifiesta un informe.[6] El día 7 de enero de 2001, varias compañías no identificadas concretaron la formación de la Alianza Estratégica de la Red-C de China, la cual es una red de segunda generación parecida al Internet para los sectores gubernamental e industrial del país. Aún no se han fijado las fechas para iniciar y completar su construcción. En un comunicado de la Agencia Noticiera de Xinhua se observa que "el [Internet] actualmente en existencia ostenta demasiadas fallas y es incapaz de cumplir con las exigencias del Gobierno y de las industrias de China, a medida que entran de lleno la era de la digitalización. Aún no se sabe si los extranjeros tendrán acceso o no a la red, o si ésta será compatible con la red ya existente".[7]

Estrategia Informática en *China Military Science*

La publicación, *China Military Science*, es una revista militar publicada trimestralmente que, durante el año pasado, sirvió como foro limitado para la publicación de

artículos sobre guerra/operaciones de información. Sin embargo, el número de abril de 2000 fue una excepción, por cuanto salieron en dicha revista tres importantes artículos sobre temas relacionados con guerra/operaciones de información. El primero, titulado "The Current Revolution in Military Affairs and Its Impact on Asia-Pacific Security" (La actual revolución en los asuntos militares y su impacto en la seguridad de Asia Pacífico), fue escrito por el coronel Wang Baocun, un respetado autor sobre temas de informática que cumple funciones en el Departamento de Estudios Militares Extranjeros de la Academia de Ciencias Militares, entidad responsable de editar dicha publicación. El artículo del coronel Wang es el único escrito en inglés en este número y refleja una perspectiva occidental de la guerra de información y de la revolución en asuntos militares. Por ejemplo, Wang define la guerra de información como "una forma de acciones de combate que ataca la información y los sistemas de información del enemigo, al mismo tiempo que protege los de la fuerza propia. El contenido de la guerra de la información comprende la seguridad militar, el engaño militar, el ataque físico, la guerra electrónica, la guerra psicológica y la guerra cibernética, con el objeto fundamental de ganar y mantener el control de la información".[8]

Wang propuso una definición muy distinta de la guerra de la información cuando escribió otro artículo para la misma revista en el año 1997. Su descripción en ese escrito incluía elementos de la ciencia militar soviética/rusa, relativos a la naturaleza, las formas, los niveles, las distinciones, las características y los principios de la guerra de la información. Wang identificó los tiempos de paz, de crisis y de guerra como las formas de la guerra de información; su naturaleza se refleja en las operaciones ofensivas y defensivas; los niveles de la guerra de información son el nacional, el estratégico, el táctico y el de teatro; y las demás distinciones de la guerra de la información se encuentran en los ámbitos de comando y control, inteligencia, dimensiones electrónica-psicológicas, el ciberespacio, las actividades de *hackers*, la realidad virtual, aspectos económicos, estrategia y precisión. Enumeró las siguientes características de la guerra de la información: complejidad, objetivos limitados, corta duración, menos daños físicos, mayor espacio de combate y menor densidad de tropas, transparencia, lucha intensa por la superioridad de la información, aumentada integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas y el hecho de que el enemigo efectivo tal vez no sea el objetivo principal. Afirmó que los principios de la guerra de la información incluyen la "decapitación", acciones cegadoras, la transparencia, la reacción rápida y la supervivencia.[9]

Las dos definiciones propuestas por Wang reflejan dos posibles percepciones de la guerra de la información en China. La primera definición es a través del prisma de la teoría occidental, en tanto que la segunda se observa a través de la óptica de la ciencia militar soviética/rusa, la cual se empleó extensamente desde la década de los años 50 hasta principios de los años 90. En sus recientes conferencias, Wang ha mencionado la "guerra informacionalizada", un concepto empleado por Dai con gran frecuencia en su artículo.[10]

El artículo "On Information Warfare Strategies" (De las estrategias de la guerra de la información), por el general de división Niu Li, el coronel Li Jiangzhou y el mayor Xu Dehui del Instituto de Comunicaciones y Comando, apareció en el mismo número de abril 2000. Los autores definen las estratagemas de la guerra de la información como "trucos y métodos concebidos y empleados por comandantes y por entidades directivas para tomar y mantener la supremacía de la información, a través del empleo de métodos inteligentes para prevalecer a un costo relativamente bajo en la guerra de la información".[11] Los líderes chinos opinan que es posible elaborar estratagemas que les permitirán contrapesar su inferioridad tecnológica, mediante la combinación adecuada del pensamiento cualitativo del ser humano con los cálculos cuantitativos facilitados por computadoras. Los autores recomiendan que se conciban estratagemas basadas tanto en el conocimiento humano como en la tecnología (es decir, en la adquisición y procesamiento de información).

Los asiáticos no comparten la perspectiva comúnmente defendida en Occidente, respecto de la combinación de estratagemas con tecnologías. Los autores del referido artículo observan que, "Tradicionalmente los pueblos orientales enfatizan estratagemas y los occidentales le atribuyen mayor énfasis a la tecnología. . . Los soldados occidentales buscan una solución tecnológica cuando enfrentan un problema, en tanto que los orientales pretenden concebir estratagemas que les permitan superar sus deficiencias tecnológicas sin cambiar las condiciones tecnológicas imperantes. El modo de pensar tradicional de los soldados orientales no fomenta el desarrollo tecnológico, aunque sí puede servir como medio eficaz para descubrir una manera de sobrevivir en una situación peligrosa".[12] Las estratagemas de la guerra de la información pueden lograr lo siguiente:

- Orientar el modo de pensar de los comandantes, obligándoles a cometer errores atacando los sistemas cognoscitivos y de creencias.
- Generar gran presión psicológica, empleando la intimidación para señalar la victoria inevitable mediante la concentración de las fuerzas y la coordinación de las redes de información.
- Intimidar a través de la demostración de las capacidades propias.
- Adoptar medidas activas y eficaces para generar sorpresa, y emplear equipo técnico y medios decisivos de la guerra de información.
- Desarrollar y ocultar las "armas mortíferas" de la guerra de la información.

- Encubrir la realidad mediante la creación de una realidad ficticia.
- Aplicar simultánea o consecutivamente diversas estratagemas de engaño.
- Emplear todos los medios de la guerra de la información para mantener la supremacía.
- Fingir conformidad con los deseos del enemigo.
- Propagar virus computacionales para contaminar el flujo de la información.
- Controlar los elementos temporales mediante la conducción de iniciativas en el ámbito de la información tendientes a "inducir", "engañar", "encubrir", y "contener".[13]

Estas estratagemas se han diseñado para forzar al enemigo a cometer errores cognoscitivos y obligarlo a enfrentar una amenaza multidimensional.

Dai y las Estrategias en las Operaciones de Información y la Guerra Popular

El tercer artículo de interés en el número de abril de 2000 de la referida revista es "Innovating and Developing Views on Information Operations" (Innovación y Evolución de las Opiniones de las Operaciones de Información), del general Dai. En él define una operación de información de la siguiente manera: "una serie de operaciones realizadas en el ámbito de información como condición básica del campo de batalla, dirigidas a la información militar y sistemas de información como objetivo operacional directo, y adoptando la guerra electrónica y redes de computadoras como la forma principal".[14] Debido a que estas operaciones ponen a prueba las aptitudes de los partidos involucrados, enfocándose en sus conocimientos y estrategias, Dai recomienda un "enfoque en las estrategias".

Producto de los adelantos científicos y tecnológicos, las estrategias actualmente se desarrollan en un nuevo campo de batalla. Una estrategia puede implicar diferentes contenidos bajo diferentes condiciones tecnológicas, situación que permite la implementación de algunas estrategias tradicionales y de otras nuevas, posibilitadas por los nuevos medios tecnológicos. Las opciones incluyen nuevas estrategias de información/confrontación, agregando aspectos estratégicos a la tecnología en existencia y aplicando estrategias que permitan aprovechar la tecnología.[15] Si la tecnología se manifiesta en armas y equipo, entonces los sistemas de información e incluso los electrones pueden llegar a

constituir un vehículo para la estrategia. Una buena estrategia puede "servir como una especie de capacidad de lucha invisible; puede contrapesar, en cierta medida, la insuficiencia de materiales; puede disminuir una disparidad tecnológica o material entre un ejército y su enemigo; y puede compensar la escasez de información y de fuerzas de combate o una inferioridad de medios para la conducción de operaciones de información".[16] Algunas de estas estrategias son las siguientes:

- Interrumpir o sabotear la información o el sistema de información del enemigo.
- Sabotear la estructura del enemigo para la conducción de operaciones de información.
- Debilitar la capacidad del enemigo para contrarrestar una ofensiva de información.
- Dispersar las fuerzas, armas y fuegos del enemigo, logrando al mismo tiempo la concentración de las fuerzas, armas y fuegos de las unidades propias.
- Confundir o efectuar diversión al enemigo, creando una excelente oportunidad de combate para la fuerza propia.
- Efectuar diversión sobre las actividades enemigas en el ámbito de reconocimiento y realizar los preparativos adecuados para los elementos propios.
- Comunicar información falsa al enemigo y lanzar simultáneamente un ataque sorpresivo de información.
- Crear impresiones falsas para cegar o ensordecer al enemigo.
- Confundir al enemigo o interrumpir su pensamiento.
- Persuadir al enemigo de que lo real es falso y lo falso es real.
- Incitar al enemigo a tomar una decisión errónea o bien realizar una acción equivocada. [17]

Dai destaca también la necesidad de lograr la integración de todos los medios disponibles en las operaciones del futuro. Por ejemplo, deberán integrarse los elementos civiles y militares empleados en misiones de información. Dai es de opinión que los sistemas de información brindan más oportunidades para aumentar la cantidad de personas participantes en las operaciones de información, y que estas personas servirán como una importante fuerza de combate en una futura guerra de información.[18] La integración de especialistas civiles y militares revitalizará la teoría de la guerra popular elaborada por Mao Zedong, tal como observó el especialista en guerra de información de China, el general Wang Pufong, en el año 1995.[19]

Las ideas para unir el concepto de una guerra popular con la guerra de la información encuentran terreno fértil entre los 1,5 millones de efectivos de la fuerza de reserva de China. Varias fuerzas de la reserva ya se han formado en las ciudades de Datong, Xiamen, Shanghai, Echeng y Xi'an. Cada una también está perfeccionando su propia especialización. Por ejemplo, las fuerzas de reserva en Shanghai se están concentrando en el uso de redes de telecomunicaciones inalámbricas y en contraseñas de doble código.

En Xi'an, el Departamento de las Fuerzas Armadas Populares está formulando varias estrategias basadas en la idea de Dai, para convertir la luz, el sonido y la electrónica en medios estratégicos. En un ejercicio realizado en el distrito militar en la provincia de Jilin (Región Militar de Shenyang) se emplearon unos *Fenduis* (divisiones) especializados en la guerra electrónica en función de fuerza adversaria. De esa experiencia se derivaron los siguientes diez métodos para la conducción de operaciones electrónicas, los cuales también pueden ser considerados como estrategias electrónicas:

- Sembrar "minas" de información.
- Conducir misiones de reconocimiento para obtener información.
- Cambiar los datos en las redes.
- Lanzar "bombas" de información.
- Desechar toda información inútil.
- Diseminar propaganda.
- Aplicar estratagemas de engaño en el ámbito de la información.
- Divulgar información redundante.
- Organizar la defensa de la información.
- Establecer estaciones de espionaje en la red.[20]

No se sabe si estas estrategias actualmente se emplean o no en misiones de reconocimiento externo de los sistemas de operaciones de países extranjeros.

La tercera forma importante en que la era de la información ha afectado la actitud de China en relación con la conducción de la guerra, es que sus 36 estratagemas pueden adquirir nuevos significados y encontrar nuevas aplicaciones. Hace aproximadamente 300 años, un erudito desconocido tomó la decisión de recolectar y registrar las estratagemas elaboradas por China. Su obra, *The Thirty-six Stratagems: The Secret Art of War* (Las treinta y seis estratagemas: El arte secreto de la guerra), subraya la importancia del engaño como arte militar capaz de lograr objetivos militares.[21] En la actual era de la información, caracterizada por ataques anónimos e incertidumbre, esta estratagema quizás se revitalice como una táctica capaz de facilitar a los elementos propios engañar al adversario o, cuando menos, dificultarle precisar sus percepciones (errores de guía, en chino). La era de la información se está tornando en la era del convencimiento anónimo.

Algunos sostienen que en el mundo moderno de la alta tecnología, estas estratagemas ya no tienen aplicación. Sin embargo, con echarle un vistazo solamente a las cinco estratagemas iniciales, resulta obvio que no es así. La primera estrategia implica "engañar al emperador para poder atravesar el mar".[22] Hacer que el enemigo disminuya su vigilancia debe ser un acto abierto, ocultando las verdaderas intenciones bajo el manto de las actividades cotidianas. Una aplicación de la guerra electrónica implicaría, por ejemplo, el empleo de los servicios comunes de correo electrónico y

de diversos enlaces en Internet para disimular la introducción de códigos dañinos o bien de algún virus computacional. La segunda estrategia es la de "sitiar a Wei para rescatar a Zhao"; o sea, cuando el enemigo no puede ser vencido en un ataque directo, hay que atacar algo que para él tenga gran valor. La implicancia de la guerra de la información de hoy en día es que, cuando no es posible atacar a un adversario con armas nucleares debido a los efectos catastróficos producidos por tal ataque en la propia patria, hay que desatar los electrones en un ataque contra los servidores y redes responsables de mantener la estabilidad de los sistemas financieros, eléctricos y políticos de Occidente. La tercera estrategia es "dar muerte con una espada prestada": en ausencia de los medios requeridos para atacar al enemigo en forma directa, debe ser atacado con los de otra potencia. La aplicación en el ámbito de la guerra de la información en sencilla: transmitir códigos y virus dañinos a través del sistema computacional de otro partido o país.

La cuarta estrategia es "esperar con calma al enemigo exhausto": es ventajoso estar en condiciones de seleccionar el momento y el lugar de la batalla. De ahí que se deba estimular al enemigo para que gaste su energía en acciones inútiles, conservando al mismo tiempo la fuerza propia. Cuando el enemigo quede rendido y confundido, debe ser atacado con energía y resolución. La aplicación de la guerra electrónica en este sentido gira en torno al empleo de la teoría de la guerra popular para lanzar múltiples ataques, siempre conservando el ataque principal hasta tal momento que todos los equipos de reacción en casos de emergencias computacionales se encuentren ocupados. Finalmente, la quinta estrategia aconseja "saquear una casa en llamas": cuando un país es azotado por problemas internos, no estará en condiciones de contrarrestar una amenaza del exterior. La aplicación en el ámbito de la guerra de la información es desplegar a *hackers* —expertos en la tecnología de la informática— en los países occidentales, disfrazados de estudiantes o comerciantes, con la misión de atacar desde adentro. Mientras predomina el caos, estas personas deberán saquear los medios de la información.

La integración también implica el empleo de redes. En un artículo publicado en un diario en el mes de agosto de 2000, con el título, "PRC Army Pays Attention to the Role of Network Warfare" (El Ejército de la República Popular China Presta Atención al Papel de la Guerra de Redes Electrónicas), una guerra popular recibió tanta atención como la manipulación de redes electrónicas. El autor aseveró que el diario de las Fuerzas Armadas chinas, *Jiefangjun Bao*, insiste en la necesidad de formular las reglas y los reglamentos adecuados para la movilización y preparación para una "moderna guerra popular", como también para la obtención y procesamiento de información; acciones ofensivas y defensivas en Internet; e investigaciones e intercambios de tecnología de las redes computacionales, para así establecer las normas necesarias para la preparación del desarrollo de una "guerra popular vía redes computacionales".[23]

El logro de la superioridad de la información (Dai emplea tal término 32 veces y se refiere al concepto del "control de la información" 11 veces en su artículo) es un elemento vital en el empleo de estas estrategias en una guerra popular e implica varias etapas. Primero, Dai observa que las fuerzas profesionales (posiblemente el Ejército de Liberación Popular) habrían de obtener, transmitir y procesar la información sobre la guerra, interrumpiendo o saboteando simultáneamente la información o sistemas de información del enemigo. Las fuerzas no profesionales (tal vez los elementos de reserva) protegen blancos específicos e infligen daños a la fuerza efectiva del enemigo. Segundo, los medios de guerra electrónica (diseñados para sabotear capacidades de recolección y transmisión de información) y los medios de guerra de las redes electrónicas (diseñados para sabotear el procesamiento y uso de información) deben ser combinados. Tercero, los términos "blandas y duras" deben describir tanto a las fuerzas como las operaciones ofensivas y defensivas.[24] La ofensiva incluye unidades especializadas en la electrónica, en el uso de redes y otras empleadas para destruir los sistemas electrónicos del enemigo; la

El artículo "On Information Warfare Strategies" (De las estrategias de la guerra de la información), por el general de división Niu Li, el coronel Li Jiangzhou y el mayor Xu Dehui del Instituto de Comunicaciones y Comando, [señala que] . . .Los asiáticos no comparten la perspectiva comúnmente defendida en Occidente, respecto de la combinación de estratagemas con tecnologías. Los autores del referido artículo observan que, "Tradicionalmente los pueblos orientales enfatizan estratagemas y los occidentales le atribuyen mayor énfasis a la tecnología. . . Los soldados occidentales buscan una solución tecnológica cuando enfrentan un problema, en tanto que los orientales pretenden concebir estratagemas que les permitan superar sus deficiencias tecnológicas sin cambiar las condiciones tecnológicas imperantes. El modo de pensar tradicional de los soldados orientales no fomenta el desarrollo tecnológico, aunque sí puede servir como medio eficaz para descubrir una manera de sobrevivir en una situación peligrosa".

La conclusión principal sacada de una revisión de las estratagemas chinas en el ámbito de la guerra de información es que la estrategia, el arte militar y la ciencia de la conducción de campañas en amplia escala se han sometido a un proceso de transformación. Grandes concentraciones de fuerzas serán reemplazadas por la eficacia de asaltos lanzados con información y energía, al mismo tiempo que las distinciones entre el frente y la retaguardia se harán borrosas. Las operaciones dejarán de enfatizar la potencia de fuego para destacar más bien actividades de detección, encubrimiento, búsqueda y evasión, dando como resultado que el combate desde largas distancias reemplace al combate cercano.

defensa consiste en unidades de telecomunicaciones, reconocimiento técnico, radares y otras. Cuarto, las operaciones integradas, conjuntas y multidimensionales deben materializarse en el mar, el aire y el espacio.[25]

Dai comenta que competir por la superioridad de la información exige ver las operaciones de información como una "ofensiva activa". Esta opinión parece contradecir la perspectiva plasmada subsecuentemente en el Libro Blanco sobre la Defensa de China, que hizo hincapié en la adhesión de dicho país a una postura de defensa activa. Sin embargo, Dai observa que una defensa positiva tiene que ser una "defensa basada en una ofensiva activa", en tanto que una defensa basada en información negativa será pasiva. Tal juego de palabras parece haberse concebido con el fin de mantener el concepto de la "ofensiva activa de la información" en consonancia con el Libro Blanco.[26] En este sentido, Dai recomienda el modelo establecido por los serbios en Kosovo como ejemplo de una respuesta activa, antes que el de los iraquíes durante la Guerra del Golfo Pérsico, que esperaron pasivamente para que la coalición iniciara la acción.

Otras Estrategias de la Información

Un artículo publicado en el año 1996 señala que la tecnología de la información es la esencia y el cimiento de la revolución militar. La información y el conocimiento han cambiado el método anteriormente existente para medir la potencia militar, la que anteriormente se calculaba contando las divisiones blindadas, escuadrillas aéreas y grupos de portaaviones. Hoy en día es imprescindible incluir fuerzas invisibles en el cómputo de la correlación de fuerzas. Estas fuerzas incluyen:

- Capacidades de computación, incluyendo rendimiento total.
- Capacidad y volumen de comunicaciones.
- Fiabilidad de los sistemas.
- Capacidad de los sistemas de reconocimiento.[27]

Cada elemento puede afectar la estrategia de información empleada por un eventual adversario, como asimismo la información empleada en su contra. Estas estrategias también tienen un alcance global, son capaces de transmitir datos a la velocidad de la luz y logran la completa integración de medios.

Además, resulta necesario evaluar los conocimientos y los factores psicológicos como componentes de la correlación de fuerzas. La guerra del conocimiento implica calcular los cambios importantes en poblaciones, armas y sistemas militares. El impacto de una disparidad de conocimientos fue claro entre los soldados estadounidenses y los iraquíes en la Guerra del Golfo Pérsico. Las armas de la más alta tecnología empleadas por la coalición no les habría servido a los soldados iraquíes, muchos de los cuales eran analfabetos. La guerra del futuro, caracterizada por una competencia tipo ajedrez y por conocimientos de alta tecnología integrados en los circuitos de armas, será "dirigida por oficiales con títulos de posgrado, comandada por estudiantes universitarios y conducida por expertos". Es más, la conversión de conocimientos en sistemas de armas ocurrirá en forma más rápida. Se producirán mejoras en cuanto a la competencia en el uso de redes, la automatización y sistemas que funcionan en tiempo real para fines de alerta temprana, control y orientación, reconocimiento y ataque, permitiendo que las armas identifiquen, diferencien y analicen objetivos en forma automática. Los sistemas militares reemplazarán los aspectos de cantidad y escala con los de calidad y eficacia.[28] La guerra del conocimiento también incluye el desarrollo de estrategias superiores basadas en conocimientos superiores.

La conclusión principal sacada de una revisión de las estratagemas chinas en el ámbito de la guerra de información es que la estrategia, el arte militar y la ciencia de la conducción de campañas en amplia escala se han sometido a un proceso de transformación. Grandes concentraciones de fuerzas serán reemplazadas por la eficacia de asaltos lanzados con información y energía, al mismo tiempo que las distinciones entre el frente y la retaguardia se harán borrosas. Las operaciones dejarán de enfatizar la potencia de fuego para destacar más bien actividades de detección, encubrimiento, búsqueda y evasión, dando como resultado que el combate desde largas distancias reemplace al combate cercano. Un aspecto central será la lucha por lograr la supremacía de las redes electrónicas, la cual será indispensable para lograr simultáneas victorias en los niveles estratégico y táctico.

En un avance revolucionario, será posible desplegar "nubes" de electrones para incapacitar y destruir países enteros (normalmente mediante la destrucción económica, pero también vía ataques informacionales/psicológicos), en lugar de comprometer a las grandes fuerzas anteriormente requeridas para lograr el mismo fin. Los electrones y las tecnologías informáticas son las nuevas formaciones de las fuerzas armadas del siglo XXI en China y en otros países. Los electrones en combate exigen un enfoque en la eficacia operacional en lugar de una concentración de la potencia militar. De acuerdo con algunos analistas de asuntos chinos, el desarrollo de sistemas capaces de efectuar la destrucción "blanda" del enemigo (a través del engaño o bien de la interrupción de señales) asumirá tanta importancia como la potencia de fuego. Occidente deberá estudiar Oriente para entender estas estratagemas. Tal como observan los propios chinos, ellos dedican más tiempo que sus homólogos occidentales al pensamiento estratégico.

Existen unas nuevas áreas de énfasis que apoyan estas estrategias, incluyendo los nuevos criterios para calcular la correlación de fuerzas y el nuevo énfasis en factores cognoscitivos, especialmente psicológicos. Para China, la revolución en el ámbito de la información ha revitalizado una estrategia antigua sin embargo oportuna: la guerra popular. El país puede unificarse en torno a tal concepto, incluyendo a sus fuerzas de reserva y cualquier persona que posea una computadora portátil. Para los observadores occidentales, ya es tiempo de estudiar minuciosamente estos cambios y resolverse a adaptar algunos en nuestro modo de conducir la guerra de información. ***MR***

NOTAS

1. Quingmin Dai, "Innovating and Developing Views on Information Operations", Beijing *Zhongguo Junshi Kexue* (20 de agosto de 2000), págs. 72-77. Traducido y bajado del Servicio de Información de Transmisiones Extranjeras, 9 de noviembre de 2000, http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.
2. El Informe al Congreso Conforme al Acta de Autorización de la Defensa Nacional del Año Fiscal 2000, www.defenselink.mil/news/Jun2000/china06222000.htm.
3. Zhang Fuyou, "With Joint Efforts Made by Army and People, Military Telecommunications Makes Leap Forward", Beijing *Jiefangjun Bao* (9 de septiembre de 2000), Traducido y bajado del Servicio de Información de Transmisiones Extranjeras, http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.
4. *Ibíd.*
5. El Informe al Congreso.
6. Wei Kaqing, "On the Sudden Emergence of Military Websites", Beijing *Zhongguo Guofang_Bao* (6 de noviembre de 2000), pág. 4. Traducido y bajado del Servicio de Información de Transmisiones Extranjeras (14 de diciembre de 2000), http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.
7. Beijing, *The Associated Press* (8 de enero de 2001).
8. Wang Baocun, "The Current Revolution in Military Affairs and Its Impact on Asia-Pacific Security", *China Military Science* (abril de 2000), pág. 139.
9. Baocun, "A Preliminary Analysis of IW", Beijing *Zhongguo Junshi Kexue* (20 de noviembre de 1997), págs. 102-11. Traducido y bajado del Servicio de Información de Transmisiones Extranjeras, http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.
10. *Ibíd.*
11. Niu Li, Li Jiangzhou y Xu Dehui, "On Information Warfare Stratagems", Beijing *Zhongguo Junshi Kexue* (12 de enero de 2001), págs. 115-22. Traducido y bajado del Servicio de Información de Transmisiones Extranjeras, http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.
12. *Ibíd.*
13. *Ibíd.*
14. Dai, "Innovating and Developing Views on Information Operations".
15. *Ibíd.*
16. Ibíd.
17. *Ibíd.*
18. Ibíd.
19. Wang Pufeng, "Meeting the Challenge of Information Warfare", *Zhongguo Junshi Kexue* (20 de febrero de 1995), págs. 8-18. Traducido y publicado en el Servicio de Información de Transmisiones Extranjeras, FBIS-CHI-95-129 (6 de julio de 1995), págs. 29 y 30.
20. *Xianjin Bao* (10 de diciembre de 1999); enviado vía correo electrónico al autor por el Sr. William Belk.
21. Wang Xuanming, *The Thirty-Six Stratagems: The Secret Art of War* (China Books and Periodicals, diciembre de 1992).
22. Estas estrategias y su significado fueron bajados del sitio http://www.chinastrategies.com; la interpretación desde la perspectiva de la era de la información es del autor.
23. "PRC Army Pays Attention to the Role of Network Warfare", Hong Kong *Zhongguo Tonnxun She* (6 de agosto de 2000), traducido y bajado del Servicio de Información de Transmisiones Extranjeras, http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.
24. Dai. "Blando" significa sabotaje o destrucción temporal empleando técnicas tales como la interferencia electrónica, ataques de virus computacionales, infiltración de redes, bombas de fibras carbonizadas, ataques de realidad virtual y ataques psicológicos. "Duro" se refiere a acciones de sabotaje permanente, debilitamiento de la capacidad de lucha total de un adversario e incluye armas convencionales, ataques con fuerzas con fines de sabotaje, ataques con impulsos electromagnéticos y ataques con buscadores de aparatos orientadores de portaarmas.
25. *Ibíd.*
26. *Ibíd.*
27. Hai Lung y Chang Feng, "Chinese Military Studies Information Warfare", *Kuang Chiao Ching* (16 de enero de 1996), págs. 22 y 23. Traducido en FBIS-CHI-96-035, 21 de febrero de 1996, págs. 33 y 34.
28. Jia Xi y Shi Hongju, "Analysis on Key Elements of Knowledge Warfare", Beijing *Jiefangjun Bao* (18 de septiembre de 2000). Traducido y bajado del Servicio de Información de Transmisiones Extranjeras, http://sun3.lib/uci.edu/-sica/microform/resources/f-g/f_049.htm.

El teniente coronel Timothy L. Thomas, retirado del Ejército de EE.UU., es analista en la Oficina de Estudios Militares Extranjeros, en el Fuerte Leavenworth, en Kansas, sirviendo además como profesor adjunto en el Instituto Europeo-Asiático del Ejército de EE.UU., localizado en Garmisch, Alemania. Recibió el grado de Bachiller en Ciencias de la Academia del Ejército de EE.UU., en West Point, el de Maestría en Artes en la Universidad de California del Sur, y es graduado de la Escuela de Comando y Estado Mayor del Ejército de EE.UU. y del Instituto Ruso del Ejército de EE.UU. Ha prestado servicios en varias posiciones de mando y estado mayor en el territorio continental de Estados Unidos y en Europa, incluyendo como Director del Departamento de Estudios Soviéticos del Instituto Ruso del Ejército de EE.UU., en Garmisch; inspector de las operaciones tácticas soviéticas, en la Conferencia de Seguridad de Cooperación en Europa, en el Instituto Europeo-Asiático en Garmisch, Alemania; y como S2, 2ª Brigada, y comandante de la Compañía C, 313º Batallón de Inteligencia Militar, 82ª División de Paracaidistas, Fuerte Bragg, Carolina del Norte. Es editor asistente de la revista, European Security. Su artículo, "Grozny 2000: Urban Combat Lessons Learned", apareció en el número de julio-agosto de 2000 de Military Review, *edición en inglés.*